UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/809,507	03/26/2004	Ryogo Yanagisawa	2004-0472A	8594

52349 7590 09/17/2008

WENDEROTH, LIND & PONACK L.L.P.
2033 K. STREET, NW
SUITE 800
WASHINGTON, DC 20006

EXAMINER	
WANG, HARRIS C	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
09/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/809,507	YANAGISAWA, RYOGO	
	Examiner	Art Unit	
	HARRIS C. WANG	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 July 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-7,9-11,13-16 and 18-23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-3, 5-7, 9-11, 13-16, 18-2* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-3, 5-7, 9-11, 13-16, 18-23 are pending

2. Claims 20-23 are new

3. Claims 4, 8, 12, 17 have been cancelled.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/15/2008 has been entered.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 20-21 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to

one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The Applicant has added new claims that include the limitation "wherein the public key generator uses the random key ka in the one semiconductor integrated circuit only for the calculation of the public key ya." The Applicant has added no support for these limitations in the specification. The Examiner has found "the secret key ka is used in the chip of the semiconductor integrated circuit only for the generation of the public key ya **and** the shared key Ka (Paragraph [0039] of Applicant's specification)"

The Examiner could not find any evidence of different 'ka's being used for the calculation of the public key and the shared key.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-3, 5-7, 9-11, 13-16, 18-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding the Applicants amendment in independent claims 1, 5, 9, 13 "wherein the random number generator generates a new random number after the calculation of the public key ya is completed so that the public key ya becomes a function of the random number," the Examiner is confused on the order of the operation. If the random number is generated after the key is completed, how can the public key then become a function of the random number.

The remaining claims are dependent on the above claims and are rejected for the same rationale.

Once again the Applicant has provided no support for this new limitation. The Examiner has found "the random number generator generates a new random number ka after the calculation of the public key ya is completed. Therefore, each time the public key ya is outputted, it has a different value (Paragraph [0030] of Applicant's Specification)." The Examiner will interpret the new limitation as described in the specification for the purpose of examination.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-2, 5-6, 9-10, 13-14, 16,18-19, 21-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Goss (4956863).

Regarding Claims 1-2, 5-6, 9-10, 13-14, 16, 18-19

Goss teaches a key exchange apparatus including:

a random number generator for generating a random number ka that holds a relationship 0 < ka< q, where an element in a finite group F for which multiplication is defined is g and an order that is a prime number of the element g is q; *("The first step in establishing the session key is that each user generates a secret number in a random number generator 14, 16. The numbers are designated Xa, Xb respectively, and are selected from a set of positive integers up to p-1" Column 6, lines 23-27)*

a secret key holding unit for temporarily holding the random number ka; *("Storage area 40 contains a preselected number Xa, stored at the time of manufacture of the A device" Column 7, line 52)*

a public key generator for calculating a public key ya in the finite group F from the random number ka, the element g, and the prime number q;

$(Ya = a^{Xa} \bmod(p), Yb = a^{Xb} \bmod(p)$ *(Column 6, lines 30-35)*

and a shared key generator for calculating a shared key Ka in the finite group F using a public key yb generated from a random number kb which holds a relationship 0<kb<q and is generated by a second user as a destination distribution of the shared key, and the random number ka that is held by the secret key holding unit, *("Each user also has a session key generator 18, 20…After the exchange of values Ya, Yb, each user computers a session key K in its session key generator 18, 20 by raising the other user's Y value to the power represented by the user's own X value, all modulo p" Column 6, lines 27-28, 55-60)*

a controller of a first user as a distribution source of the shared key controlling the random number generator and the public key generator for obtaining the public key ya, and transmitting the obtained public key ya to a second user as a distribution

destination of the shared key, and said controller obtaining the public key yb from the second user as the shared key distribution destination, and controlling the shared key generator for deriving the shared key Ka. *("The key management steps previously described proceed automatically under the control of the cryptographic processor 60, and when a session key has been derived, this is automatically applied in a conventional cryptographic process" Column 12, lines 25-30)*

wherein the random number generator generates a new random number after the calculation of the public key ya is completed so that the public key ya becomes a function of the random number *("When additional numbers X'a and X'b are also generated prior to transmission, the means for generating the session key performs the transformation...where X'a is the number of the first type that is randomly generated, Y'b is the additional number of the second type" Column 4, lines 61-66) The Examiner interprets X'a and Y'b as the new random numbers generated. The new random number must be held in order to further calculate the session key described in Column 5: lines 19-27 of Goss.*

Goss does not explicitly teach where at least said random number generator, said secret key holding unit, said public key generator, and the shared key generator being formed on one semiconductor integrated circuit so as to prevent diversion or alteration of an arithmetic algorithm of the public key generator, wherein the arithmetic algorithm of the public key generator is not revealed outside of the one semiconductor integrated circuit.

Ober (US 20020080958) teaches a random number generator, secret key holding unit , public key generator, shared key generator being formed on one semiconductor integrated, wherein the arithmetic algorithm of the public key generator

is not revealed outside the semiconductor integrated circuit. *("In keeping with the philosophy of a "security system on-a-chip", the CryptIC incorporates a powerful and secure key management system into both its hardware and CGX firmware" Paragraph [0068])* *((Paragraphs [0148-0151] detail the Diffie-Hellman public key and shared key generation in the CryptIC)*

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement the method of Goss to be implemented on one semiconductor integrated circuit as taught by Ober.

The motivation is to "generate and safely store key material" (Paragraph [0076] of Ober)

The methods associated with the apparatus are taught in the cited sections.

Regarding Claim 21,

Goss and Ober teach the shared key generation apparatus of claim 5, wherein the shared key uses the random key ka in the one semiconductor integrated circuit only for the calculation of the shared key Ka. *("For user B, the computation is K = Ya^xb mod p" Column 6, lines 65-69) where Ya = alpha^xa mod p.*

Regarding Claims 22-23,

Goss and Ober teach the key exchange apparatus of claims 9 and 13. The random key "ka" is only used for the public key and shared key generation. *(See citations above and Column 6 of Goss)*

Claims 3, 7, 11, 15, are rejected under 35 U.S.C. 103(a) as being unpatentable over Goss in view of Ober further in view of Applicant Admitted Prior Art.

Regarding Claim 3, 7, 11,15,

Goss and Ober teach the key exchange apparatus of claim 13.

Goss does not explicitly teach wherein when the finite group F is an elliptic curve E(F) in a finite field, and an element on the elliptic curve E(F) is G, the public key generator calculates the public key ya on the elliptic curve E(F) using the random number ka, the element G, and the prime number q by a formula: ya=kaG mod q, and the shared key generator calculates the shared key Ka on the elliptic curve E(F) by a formula: Ka=Kayb mod q, using the public key yb=kbG mod q that is generated from the random number kb on the elliptic curve E(F) by the second user as the shared key distribution destination, and the random number ka that is held in the secret key holding unit.

Applicant admitted prior art (APA) teaches in the background of the invention "An elliptic curve crypto system is widely known as a cryptosystem based on the difficulty in solving the discrete logarithm problem in the finite group F. More specifically, when assuming an elliptic curve in the finite group as E(F) a point on the elliptic curve E(F) which is previously shared by the user 1 and the user 2 as G, and an arithmetic xG using a point x on the epplictic curve E(f) is defined."

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Goss and Ober to have the finite group F as an elliptic curve E(f) in a finite field, and an element on the elliptic curve E(f) is G.

The motivation is to provide additional security.

Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Goss and Ober in view of Official Notice..

Regarding Claim 20,

Goss and Ober teach the public key generation apparatus of claim 1. Goss and Ober do not explicitly teach that the public key generator uses the random key ka only for the calculation of the public key ya.

The Examiner takes Official Notice it would have been obvious to one of ordinary skill in the art at the time of the invention to omit the step of using "ka" for a shared key in Goss, and then the ka would only be used for the calculation of the public key.

The elimination of a step is considered an obvious modification.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HARRIS C. WANG whose telephone number is (571)270-1462. The examiner can normally be reached on M-F 9-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, KRISTINE KINCAID can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

HCW

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139